(12) UK Patent Application (19) GB (11) 2 270 446 (13) A

(43) Date of A Publication 09.03.1994

(21) Application No 9218816.8

(22) Date of Filing 04.09.1992

(71) Applicant(s)
IBM UK Ltd

(Incorporated in the United Kingdom)

PO Box 41, North Harbour, Portsmouth, Hampshire, United Kingdom

(72) Inventor(s)
Christopher J Holloway

(74) Agent and/or Address for Service
J P Richards
IBM United Kingdom Patent Operations, Hursley Park, Winchester, Hants, SO21 2JN, United Kingdom

(51) INT CL[5]
H04L 9/32 9/30

(52) UK CL (Edition M)
H4P PDCSC PDCSX

(56) Documents Cited
EP 0393806 A2 EP 0277247 A1 EP 0254812 A2

(58) Field of Search
UK CL (Edition K) H4P PDCSP PDCSS PDCSX
INT CL[5] H04L 9/30 9/32
ONLINE DATABASES : WPI

(54) Establishing a common cryptographic key at two cryptographic sites

(57) The method includes preparing a portable data processing device ("smart card") at each site having a first data record which can only be read at that site but which can be written to at any site, and a second data record which can only be written at that site but which can be read at any site, the device also containing a testable key particular to that device. Each site also creates and publishes a set of test patterns against which the authenticity of the card can be verified. Each site then creates one part of the key to be agreed upon, and a test pattern for that key part. The test pattern is written to the site's own smart card in the second data record. The cards are exchanged, and the received cards are tested for authenticity using the published test patterns. Once accepted as genuine, the test pattern for the key part of the other site is read and stored. The key part previously generated is written onto the first data record of the received card. The cards are exchanged again. The key part is read at the home site of the card. The key part is verified for authenticity against the stored test pattern which was received earlier. Each site then combines the received key part with the locally created key part and they now share a common key.

GB 2 270 446 A

2270446

IMPROVEMENTS IN CRYPTOGRAPHY

This invention relates to a method of establishing a common cryptographic key at two cryptographic sites.

In general, cryptography has used three main forms of algorithm: Hashing Algorithms - these are one way functions which require no secret keys to be distributed.

Public Key Algorithms - these are asymmetric key systems which have the advantage for the initial distribution of keys that the distributed key may be published. As there is no requirement for secrecy, initial keys may be exchanged between previously unknown systems without the need for a channel of secrecy (for example trusted couriers).

Symmetric Key Algorithms - these algorithms require that the same secret key is held by both the sender and receiver of messages. The exchange of of initial secret keys between previously unknown systems has in the state of the art always been relatively expensive, because it has required a channel of secrecy as well as of integrity to exchange these initial keys.

It has been proposed that by providing public key cryptography to manage the initial keys of symmetric key algorithms, the problem of key exchange may be addressed. However, this requires a system supporting both algorithms in a closely integrated and secure environment, commonly known as a hybrid scheme.

It is therefore an object of this invention to provide a new approach to the distribution of initial symmetric keys that does not require the use of hybrid cryptographic systems or trusted couriers.

This object is attained by the method claimed in claim 1.

The invention provides a substantial reduction in the cost of the initial key establishement for symmetric key systems, especially when implemented using cryptographic products which are already available on the market, and using only publicly available services for the carriage

of information such as the press or the regular mail services, or such business meetings as would have been necessary for the establishment of prerequisite contracts.

An embodiment of the invention will now be described. The embodiment can (but need not) be implemented using IBM Transaction Security System products which are the IBM 4753 Network Security Processor which attaches to an central host computer running the IBM MVS Operating System, the IBM 4755 Cryptographic Adapter card, which resides inside a Personal Computer supporting the AT-Bus or Microchannel architecture and running the DOS or OS/2 operating systems, the IBM 4754 Security Interface Unit which can attach to either of the foregoing to provide secure communications with the IBM Personal Security card which is a so-called "smart" card with secured data storage and cryptographic processing capability. The IBM Personal Security Card and the IBM 4753, 4754 and 4755 each have secure storage for encryption keys and cryptographic processing capability.

In the embodiment it is assumed that each site on which cryptography must run has established a fully operational cryptographic environment supporting a key management application and hardware facilities necessary to support the scheme. Such a system may have been set-up locally or via a central initialisation facility. Neither site need have any prior knowledge of the other site, but each supports the following:

1. Common Symmetric Key Algorithm Support - both sites support the same symmetric algorithm. The Data Encryption Algorithm or DEA is a standardised and widely used symmetric algorithm.
2. Key Part Loading - in most DEA systems, initial keys are loaded into the system by providing two or more clear parts. These are either concatenated or exclusive-ORed (XORed) together. It is assumed that a common mechanism is supported at both sites.
3. Key Test Algorithm - both sites support a common method to test the true value of an installed key. The algorithm should not provide a channel of attack to discover the true key value. The key test is available in two parts, the first to generate a pattern from an installed key, the second to verify a pattern against an installed key. The

mechanism is available for testing key parts as well as completed keys. Such an algorithm is exemplified by the IBM TSS Key Test verb.

4. A Secure Portable Data Processing Device - such would be typified by a smart card, but other possibilities exist. The description uses "smart card" in this generic sense. Smart cards are used as the transport mechanism, and are interchangeable between the two sites. The IBM Personal Security card may be used and has the following functions:

a. Access Control - functions performed on the smart card may be selectively and independently controlled such that some are publicly available, and some require that the smart card authenticates the user. Publicly available means available both without user authentication, and without restriction as to which site the card is attached at the time.

b. User Authentication - this is securely performed for users of the smart card by any means deemed adequate (eg PIN or Signature).

c. Site Restriction - user authentication is restricted on the smart card to being available only at the "home site" of the smart card. This restriction is preferably be enforced by a random two way cryptographic challenge.

d. Data Access Control - a first data record on the smart card is capable of being defined such that it requires user authentication to allocate, read, delete or clear the data record; but writing to the data record is a publicly available function. A second data record on the smart card is capable of being defined such that it requires user authentication to allocate, write, delete or clear the data record; but reading the data from the record is a publicly available function.

e. Testable Key Register - a key register on the smart card contains a testable key that cannot be exported from the smart card. The Key Test function is publicly available. For the IBM Personal Security card the register is the smart card's Master Key register.

5. Site Access Control - each site is capable of access control to its cryptographic facilities independently of the use at the site of an

'alien' smart card (that is one which is unknown to the site). Such control could be by means of a previously entered "home" smart card.

There are several steps to the method, which are the same at both sites. The method is therefore described from the perspective of just one of the sites.

Each step of the mechanism is described in more detail below. In brief, however, each site creates a smart card with the properties described above with their two data records and a testable key in place. Each site also creates a set of test patterns which may be published and against which the authenticity of the card itself can be verified by the other party. Each site then creates one part of the key to be agreed upon, and a test pattern for that key part. The test pattern is written to the site's own smart card in a data record that can be written only by this site but read publicly (so that it is accessible to the other site). The cards are exchanged through the mail or via any other suitable means. The received cards are tested for authenticity using the published test patterns. Once accepted as genuine, the test pattern for the key part of the other site is read and stored. The key part previously generated is written onto a data record of the received card; this data record allows public writing but restricts reading to the receiving site. The cards are exchanged again. The key part is read at the home site of the card, this is the only site at which it can be read, and ensures secrecy of the key part. The key part is verified for authenticity against the stored test pattern which was received earlier on an authenticated card; this process ensures the integrity of the key part (that it genuinely came from the author of the test pattern). Each site then combines the received key part with the locally created key part and they now share a common key. As the key parts were created without a prior knowledge of the value of the other part, the value of the resulting key is truly arbitrary. As the verification pattern for the key part was read from an authenticated card it can be established that the key part originated from the other site. A key has been agreed between sites with full integrity and secrecy, and at low cost.

In more detail, the steps of the method are:

1. Set Up - the smart card(s) to be used for key exchange are prepared. For each smart card, a testable key is installed both on the card itself and at the owning site. A number of true key test patterns are created for the testable key. A number of false test patterns are also generated and tested to ensure that they are false. (The magnitude of "number" depends upon the degree of testing required and could be as small as two). The test patterns are published or otherwise sent to the other party.
2. Key Part Creation - a key part is created and installed on the home site. A test pattern for this part is generated and written to a secured but publicly readable first data record on the smart card. Identifiers may also be written to the smart card. A secured but publicly writable second data record is also created on the card for use at the other site.
3. Card Exchange - the smart cards are exchanged, for example through the regular mail. In this case a number of true and false test patterns would have been published. Otherwise the cards may be exchanged as a part of a contract negotiation or signing process, in which case a number of true and false test patterns could be exchanged at the same time.

Upon receipt, the card is tested by presenting true and false key test patterns. Upon request any number of further key patterns may be obtained from the correspondent by phone or mail, and tested for true or false. Similarly a number of true and false test patterns could be derived from card itself, and used to challenge the owner (again over the phone or by mail) who would use the site-installed copy of the card's key to determine which are true and which are false.

The number of such tests will be determined by the degree of certainty required that the card is genuine. The technique is well established related to 'Zero Knowledge Proof'. For 'n' satisfactory tests, the residual probability of a fake smart card is two to the power of minus 'n'.

4. Key Part Exchange - once the card has been accepted as genuine, the publicly readable second data record is read and the test pattern it holds is securely stored at the receiving site. The key part that had been locally created is then written to the publicly writable first data record on the smart card. Identifiers may also be written to the smart

card. This data cannot be read except at the smart card's own site. Its secrecy is therefore assured.

5. Card Return - the smart card(s) are then returned to their home sites, for example through the regular mail.

6. Card Reception - upon receipt the card is tested again for genuineness, by using true and false test patterns as described in step 3 above. This step distinguishes the card from any others that may be in current circulation from that site.

7. Key Part Reception - the smart card's authorised user authenticates himself to the card. The first data record is now read. The key part on the received smart card is verified against the previously stored test pattern and if good is combined with that the previously generated key part that had been dispatched on a smart card to the other site. The result is the same key at both sites.

8. Testing The Key - a final stage of verification could be applied to the combined key. This could be performed in a variety of ways. A key test could be conducted over the phone (as above), or messages exchanged across a network and protected under the key.

An initial encryption key has now been exchanged between the parties. The same process could have been used to exchange several keys, or further keys could now be exchanged over a network under the protection of the initial key.

Secrecy is preserved as the key parts can be read only at the home site. Integrity is preserved through the authentication of the card and of the key part using the key test procedure. The cost of the key exchange is minimal in comparison to traditional courier based methods.

Further restrictions regarding timeliness of the procedure could be enforced if so desired.

CLAIMS

1. A method of establishing a common cryptographic key at two cryptographic sites each supporting a common method of key testing using test patterns, comprising at each site:

(a) preparing a portable data processing device having a first data record which can only be read at that site but which can be written to at any site, and a second data record which can only be written at that site but which can be read at any site,

(b) creating a partial key and a test pattern therefor, and writing the test pattern but not the partial key into the second data record,

(c) sending the device to the other site,

(d) reading the test pattern from the second data record of the other site's device and storing it at the site,

(e) writing the partial key created at step (b) into the first data record of the other site's device,

(f) returning the other site's device to the other site,

(g) reading the partial key created at the other site from the first data record of the returned device and verifying it using the test pattern obtained at step (d), and

(h) combining the partial key created at step (b) with the partial key read at step (g) to form a full key which is the same as that formed at the other site.

2. A method as claimed in claim 1, wherein the portable data processing device also containing a testable key particular to that device, and wherein the method further comprises: between steps (a) and (b) the further step of creating a further test pattern against which the authenticity of the device can be authenticated by the other site, and making such pattern available to the other site, between steps (c) and (f) the further step of authenticating the other site's device using the

further test pattern, and between steps (f) and (h) the further step of authenticating the returned device using the further test pattern.

f ents Act 1977
Examiner's report to the Comptroller under Section 17 (The Search Report)

Application number
GB 9218816.8

Relevant Technical fields

(i) UK Cl (Edition K) HWP (PDCSS,PDCSX)

(ii) Int Cl (Edition 5) H04L 9/30, 9/32

Search Examiner
K WILLIAMS

Databases (see over)

(i) UK Patent Office

(ii) ONLINE DATABASE: WPI

Date of Search
22 OCTOBER 1992

Documents considered relevant following a search in respect of claims 1,2

Category (see over)	Identity of document and relevant passages	Relevant to claim(s)
A	EP 0393806 A2 (TRW INC) see column 6, lines 42-47	1
A	EP 0277247 A1 (K K ADVANCE) see abstract	1
A	EP 0254812 A2 (IBM) see abstract	1

Category	Identity of document and relevant passages	Relevant to claim

Categories of documents

X: Document indicating lack of novelty or of inventive step.

Y: Document indicating lack of inventive step if combined with one or more other documents of the same category.

A: Document indicating technological background and/or state of the art.

P: Document published on or after the declared priority date but before the filing date of the present application.

E: Patent document published on or after, but with priority date earlier than, the filing date of the present application.

&: Member of the same patent family, corresponding document.

Databases: The UK Patent Office database comprises classified collections of GB, EP, WO and US patent specifications as outlined periodically in the Official Journal (Patents). The on-line databases considered for search are also listed periodically in the Official Journal (Patents).